

**Объявление о проведении конкурса
по поставке межсетевых экранов нового поколения (Next-Generation Firewall).**

АКБ «Tenge Bank» объявляет конкурс на поставку межсетевых экранов нового поколения (Next-Generation Firewall).

Конкурс направлен на выбор организации по реализации межсетевых экранов нового поколения (Next-Generation Firewall) для организации периметровой защиты сети предприятия, обеспечения безопасного удалённого доступа (VPN) и централизованной фильтрации трафика.

Технические характеристики, являются минимально необходимыми (пороговыми). Участник закупки вправе предложить оборудования любого производителя, соответствующее или превосходящее указанные параметры. Указание в скобках наименований производителей или моделей не допускается; параметры сформулированы в форме, не создающей преимуществ отдельным поставщикам.

Количество поставляемых устройств, комплект ЗИП, условия гарантийного и сервисного обслуживания указываются в Спецификации (Приложение № 1), являющейся неотъемлемой частью настоящего ТЗ.

Условия участия:

Предложение необходимо предоставить во внешнем конверте с содержанием конвертов с пометками «А» и «Б». Требования ко внешнему конверту:

- Указать наименование организации.
- Указать юридический адрес и контактные данные
- Указать наименование конкурсного отбора
- Все конверты (внешний, конверт с пометкой «А», конверт с пометкой «Б») должны быть опечатаны (обязательно проставление печати фирмы) и подписаны со стороны участника отбора.

1. Конкурс открыт для всех юридических лиц, имеющих опыт в поставке межсетевых экранов нового поколения (NGFW).
2. Участники должны предоставить в конверте с пометкой «А» следующие документы:
 - Заявка на участие в конкурсе.
 - Техническое предложение, включающее характеристики и описание оборудования, которые предлагаются для поставки, а также информацию о производителе.
 - Документы, подтверждающие квалификацию и опыт работы в области поставок межсетевых экранов, включая лицензии и сертификаты на продукцию.
 - Авторизационное письмо от вендора поставляемого оборудования, что участник закупки является официальным авторизованным партнером вендора.
 - Рекомендательные письма.
 - Лицензию и свидетельство фирмы.

3. Участники должны предоставить в конверте с пометкой «Б»:

- Коммерческое предложение, в котором указана стоимость межсетевых экранов, условия оплаты, сроки поставки, гарантийный срок, способ поставки, обязательно указание уточнения наличия НДС.
- 4. Поставляемое оборудование должно соответствовать всем техническим стандартам и нормам безопасности, а также требованиям по функциональности и долговечности.
- 5. Межсетевые экраны, должны быть надежны в работе.
- 6. Технические параметры прилагаются.

При несоблюдении условий участия Конкурсная Комиссия оставляет за собой право отклонить заявку участника отбора

Крайний срок подачи коммерческих предложений: 25.08.2026 г.

Коммерческие предложения: на русском языке, оформленные в соответствии с требованиями технического задания, должны быть направлены в запечатанных конвертах, на конверте обязательно указание наименования конкурсного отбора, Конкурсной комиссии АКБ «Tenge Bank» **до 18:00 часов 25 Августа 2026 года, по адресу: г. Ташкент, улица И.Каримова 1А(Nest One блок Д) в канцелярию АКБ «Tenge Bank»**

Контактные данные: Департамент ресурсов Банка

Победитель конкурса будет определен на основе качества предложенного оборудования, стоимости, сроков поставки и гарантии. Поставщик, выигравший конкурс, получит право на поставку межсетевых экранов.

Ждем ваши заявки и предложения!

ТЕХНИЧЕСКИЕ ПАРАМЕТРЫ МЕЖСЕТЕВЫХ ЭКРАНОВ

1. Общие сведения

Предмет закупки — поставка межсетевых экранов нового поколения (Next-Generation Firewall, далее — оборудование) для организации периметровой защиты сети предприятия, обеспечения безопасного удалённого доступа (VPN) и централизованной фильтрации трафика.

Технические характеристики, приведённые в разделе 3, являются минимально необходимыми (пороговыми). Участник закупки вправе предложить оборудование любого производителя, соответствующее или превосходящее указанные параметры. Указание в скобках наименований производителей или моделей не допускается; параметры сформулированы в форме, не создающей преимуществ отдельным поставщикам.

Количество поставляемых устройств, комплект ЗИП, условия гарантийного и сервисного обслуживания указываются в Спецификации (Приложение № 1), являющейся неотъемлемой частью настоящего ТЗ.

2. Общее назначение и архитектура

- Оборудование должно представлять собой аппаратный (hardware appliance) межсетевого экран нового поколения (NGFW) в едином корпусе, без необходимости использования внешних модулей расширения для выполнения требований настоящего ТЗ.
- Поддержка отказоустойчивых режимов работы: Active/Standby и Active/Active (кластер из двух и более устройств).
- Поддержка режимов включения: L3 (маршрутизация), L2 (прозрачный/transparent), а также смешанный (гибридный) режим.
- Возможность виртуализации межсетевого экрана (виртуальные контексты / vsys / VRF) — не менее 10 логических экземпляров на одном физическом устройстве.
- Поддержка централизованного управления через выделенную платформу управления производителя (SNMP, Syslog, NETCONF/REST API или эквивалент) — обязательна.

3. Технические требования (минимальные пороговые значения)

Параметр / требование	Значение	Ед. изм.
3.1. Конструктивное исполнение		
Форм-фактор	1U, монтаж в 19" стойку	—
Габаритная высота корпуса	не более 45	мм
Встроенный твердотельный накопитель (SSD) для хранения логов/конфигурации	не менее 240	ГБ
Порт консоли управления	RJ-45 (Serial), наличие обязательно	—
Порт USB	не менее 1 × USB 3.0	—
Диапазон рабочих температур	не уже чем 0...+40	°C
Электропитание	АС 100–240 В, с резервированным блоком питания	—
Максимальная потребляемая мощность устройства	не более 250	Вт
3.2. Сетевые интерфейсы		
Порты 10/100/1000BASE-T (медь, RJ-45)	не менее 8	шт.
Порты SFP+ 1/10 Гбит/с (оптика)	не менее 4	шт.
Отдельный выделенный порт управления (Out-of-band Management)	не менее 1	шт.
Поддержка агрегирования каналов (LACP / Link Aggregation, IEEE 802.3ad)	требуется	—
Поддержка VLAN (IEEE 802.1Q)	не менее 4000	VLAN
Поддержка Jumbo-фреймов	не менее 9000	байт (MTU)
3.3. Производительность межсетевого экранирования		
Пропускная способность Stateful Firewall (пакет ≥ 1518 байт, UDP)	не менее 15	Гбит/с
Количество одновременных сессий	не менее 400 000	сессий

Параметр / требование	Значение	Ед. изм.
Количество новых соединений в секунду	не менее 50 000	соед/с
3.4. Производительность NGFW (комплексная обработка трафика)		
Пропускная способность при включённых модулях идентификации приложений (App-Control/SA) совместно с Firewall	не менее 6	Гбит/с
Пропускная способность Threat Protection (Firewall + IPS + Antivirus/AMP включены одновременно)	не менее 4	Гбит/с
Примечание к п. 3.4	см. сноску ¹ ниже	—
3.5. VPN — типы, протоколы и криптография		
Site-to-Site IPsec VPN	требуется	—
Протоколы согласования ключей	IKEv1, IKEv2	—
Remote Access VPN (клиентский удалённый доступ)	SSL VPN и/или IPsec VPN-клиент	—
Фирменный VPN-клиент производителя для Windows/macOS/Linux	требуется	—
Аутентификация VPN по сертификатам X.509 (PKI)	требуется	—
Поддержка топологий Hub-and-Spoke / Site-to-Site (множественные туннели)	требуется	—
Максимальное число одновременных Remote Access VPN-пользователей	не менее 100	польз.
Пропускная способность IPsec VPN (AES-256 / SHA-256, пакет ≥ 1024 байт)	не менее 13	Гбит/с
Максимальное число одновременных IPsec-туннелей / VPN-пиров	не менее 500	шт.
Поддерживаемые алгоритмы шифрования	AES-128/256, SHA-1/256/384	—
Пропускная способность инспекции SSL/TLS-трафика (TLS 1.2/1.3)	не менее 2,5	Гбит/с
Автоматическое получение сертификатов по протоколу SCEP	требуется	—
Perfect Forward Secrecy (группы Диффи — Хеллмана DH14 и выше)	требуется	—
Dead Peer Detection (DPD) для IPsec-туннелей	требуется	—
Проверка отзыва сертификатов (CRL и/или OCSP)	требуется	—
3.6. Функции безопасности (Security Services)		
Система предотвращения вторжений (IPS/IDS) со встроенной сигнатурной базой	требуется	—
Антивирусная проверка трафика (поточная, HTTP/FTP/SMTP/POP3/IMAP)	требуется	—
URL-фильтрация с облачной базой категорий	не менее 60 категорий	—
Идентификация и контроль приложений (Application Control / App-ID)	не менее 2000 приложений	—
Защита от DDoS-атак (SYN flood, UDP flood, ICMP flood и др.)	требуется	—

Параметр / требование	Значение	Ед. изм.
Обнаружение и блокировка ботнет-активности / C&C-трафика	требуется	—
Интеграция с песочницей (sandbox) для анализа неизвестных файлов (локально или по подписке в облаке производителя)	требуется	—
Трансляция сетевых адресов (NAT): статический, динамический, PAT	требуется	—
3.7. Маршрутизация и сетевые сервисы		
Статическая маршрутизация	требуется	—
OSPFv2 (IPv4)	требуется	—
OSPFv3 (IPv6)	требуется	—
BGP (IPv4/IPv6)	требуется	—
Policy-Based Routing (PBR)	требуется	—
Multicast-маршрутизация (IGMP, PIM)	требуется	—
Балансировка нагрузки по нескольким равнозначным маршрутам (ECMP)	не менее 4 путей	—
Защита от IP-спуфинга (Unicast Reverse Path Forwarding, uRPF)	требуется	—
Поддержка IPv6 (dual-stack)	требуется	—
DHCP-сервер и DHCP-relay	требуется	—
Клиент/сервер синхронизации времени (NTP)	требуется	—
Приоритизация и управление трафиком (QoS, traffic shaping)	требуется	—
3.8. Отказоустойчивость и SD-WAN		
Режимы кластеризации/отказоустойчивости	Active/Standby, Active/Active	—
Синхронизация состояния сессий между узлами кластера (stateful failover)	требуется	—
Встроенная функция SD-WAN с балансировкой нагрузки по нескольким WAN-каналам	требуется	—
Zero-Touch Provisioning (автоматическое первичное конфигурирование при подключении)	требуется	—
3.9. Централизованное управление (единая консоль для группы устройств)		
Единая платформа централизованного управления несколькими устройствами одного производителя (аппаратная, виртуальная или облачная)	требуется	—
Централизованное управление политиками безопасности, объектами и правилами со всех устройств из единой консоли	требуется	—
Централизованное распространение обновлений сигнатурных баз (IPS/AV/URL) на управляемые устройства	требуется	—
Централизованный мониторинг состояния устройств и событий безопасности (единая панель / dashboard)	требуется	—
Число одновременно управляемых устройств одной платформой	не менее 10	шт.
Ролевая модель доступа администраторов (RBAC) в платформе управления	требуется	—

Параметр / требование	Значение	Ед. изм.
Резервное копирование и восстановление конфигурации устройств через платформу управления	требуется	—
Локальное управление устройством (без централизованной платформы)	Web-интерфейс (HTTPS) и CLI (SSH/Serial)	—
Внешняя аутентификация администраторов	RADIUS, LDAP/AD	—
Поддержка SNMP v2c/v3	требуется	—
Экспорт журналов на внешний Syslog-сервер	требуется	—
API для интеграции с внешними системами (REST и/или NETCONF)	требуется	—
3.10. Безопасность администрирования и аудит		
Парольная политика локальных учётных записей (минимальная длина, сложность, срок действия)	требуется	—
Блокировка учётной записи после превышения числа неудачных попыток входа	требуется	—
Многофакторная аутентификация администраторов через внешний RADIUS-сервер (делегированная OTP/TOTP)	требуется	—
Журналирование (аудит) действий администраторов с привязкой к учётной записи	требуется	—
Версионирование и откат конфигурации устройства к предыдущему состоянию	требуется	—
Синхронизация времени по протоколу NTP с поддержкой аутентификации (NTP MD5/SHA)	требуется	—
Автоматическое завершение неактивной административной сессии (session timeout)	не более 15	мин.

¹ Методики измерения производительности NGFW у различных производителей отличаются размером тестового пакета и моделью трафика (фиксированный размер пакета согласно RFC 2544/3511 либо смешанная модель трафика Enterprise Mix / HTTP-объекты). При оценке соответствия заявленной производительности участника закупки заказчик принимает значение, полученное по методике производителя, при условии предоставления официального технического описания (datasheet) с указанием применённой методики тестирования.

² Требование п. 3.9 может быть закрыто отдельным программным или программно-аппаратным компонентом (сервером/виртуальной машиной) централизованного управления того же производителя, поставляемым дополнительно к устройствам и включённым в Спецификацию.

4. Требования к комплектности поставки

- Устройство в базовой аппаратной комплектации согласно разделу 3.
- Комплект монтажных креплений для установки в 19" телекоммуникационную стойку.
- Кабель питания, соответствующий стандарту электросети РУз/ПК (при необходимости — с переходником).
- Лицензии на весь заявленный функционал (Firewall, IPS, Antivirus, URL-фильтрация, App-Control, VPN) сроком не менее 36 месяцев с даты поставки.

- Лицензии и/или программный компонент централизованной платформы управления (п. 3.9) в объеме, достаточном для управления всеми поставляемыми устройствами.
- Документация на русском и/или английском языке (руководство администратора, руководство по быстрому старту).
- Обучение не менее 2 (двух) инженеров заказчика работе с поставляемым оборудованием и платформой управления на базе собственного учебного центра или курсов вендора.

5. Требования к гарантии и сервисной поддержке

- Гарантийный срок на оборудование — не менее 36 месяцев с даты подписания акта приема-передачи.
- Право на получение обновлений сигнатурных баз (IPS, антивирус, URL-фильтрация) в течение всего гарантийного периода.
- Наличие сервисной поддержки производителя или авторизованного сервисного партнера на территории Республики Узбекистан (RMA, техническая поддержка по телефону/email — 24/7/365).
- Предоставление учетной записи на портале технической поддержки вендора для самостоятельного обращения заказчика.

6. Порядок подтверждения соответствия

Участник закупки обязан представить в составе заявки официальное техническое описание (datasheet) предлагаемого оборудования, подтверждающее соответствие каждому из параметров, указанных в разделе 3 настоящего ТЗ, с указанием источника публикации (официальный сайт производителя).

Участник закупки обязан представить в составе заявки официальное авторизационное письмо от вендора поставляемого оборудования, что участник закупки является официальным авторизованным партнером вендора.

В случае отсутствия в открытых источниках данных по отдельному параметру заказчик вправе запросить у участника официальное письмо-подтверждение производит